Linear Algebra and its Applications 437 (2012) 2538–2545

Contents lists available at SciVerse ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

The cyclic groups via the Pascal matrices and the generalized Pascal matrices

Ömür Deveci *, Erdal Karaduman

Department of Mathematics, Faculty of Science and Letters, Kafkas University, 36100 Kars, Turkey
Department of Mathematics, Faculty of Science, Atatürk University, 25240 Erzurum, Turkey

ARTICLE INFO

Article history:
Received 8 December 2011
Accepted 6 June 2012
Available online 15 July 2012

Submitted by T. Laffey

AMS classification:
20F05
20D60
11A36

Keywords:
Cyclic group
Multiplicative order
Pascal matrix

ABSTRACT

In this paper, given a positive integer m, we consider the multiplicative order of upper and lower triangular matrices and symmetric matrices derived from Pascal's triangle when read modulo m. We also consider the corresponding problems when the binomial coefficients, $\binom{i}{j}$, are replaced by $x^{i-j}\binom{i}{j}$ and $x^{i+j}\binom{i}{j}$, where x is an integer satisfying certain divisibility hypotheses. We also offer some open conjectures on these orders.

1. Introduction

The Pascal matrix is an infinite matrix containing the binomial coefficients as its elements. Three different matrices – lower triangular L_n, upper triangular U_n and symmetric S_n – can hold Pascal's triangle a convenient way.

The lower triangular matrix L_n, is defined as

$$(L)_{ij} = \binom{i}{j} \quad \text{with} \quad \binom{i}{j} = 0 \quad \text{if } j > i,$$

* Corresponding author at: Department of Mathematics, Faculty of Science and Letters, Kafkas University, 36100 Kars, Turkey.
E-mail address: odeveci36@hotmail.com (Ö. Deveci).

0024-3795/$ - see front matter
http://dx.doi.org/10.1016/j.laa.2012.06.024

the upper triangular matrix U_n, is defined as

$$(U)_{ij} = \binom{j}{i} \quad \text{with} \quad \binom{j}{i} = 0 \quad \text{if } i > j,$$

the symmetric matrix S_n, is defined as

$$(S)_{ij} = \binom{i+j}{i},$$

where $i, j = 0, \ldots, n-1$. These matrices have some amazing properties. In particular, their determinants are all equal to

$$(\det\ S_n) = (\det\ L_n) = (\det\ U_n) = 1$$

and

$$S_n = L_n U_n \text{ (see[1])}.$$

For more information on these matrices, see [1,7,10].

Let x be any nonzero real number. The generalized Pascal matrix of the first kind $P_n[x]$, is defined as (see [3])

$$P_n(x; i, j) = x^{i-j}\binom{i}{j} \quad \text{with} \quad \binom{i}{j} = 0 \quad \text{if } j > i,$$

the generalized Pascal matrix of the second kind $Q_n[x]$, is defined as (see [11])

$$Q_n(x; i, j) = x^{i+j}\binom{i}{j} \quad \text{with} \quad \binom{i}{j} = 0 \quad \text{if } j > i,$$

the symmetric generalized Pascal matrix $R_n[x]$, is defined as (see [11])

$$R_n(x; i, j) = x^{i+j}\binom{i+j}{j},$$

where $i, j = 0, \ldots, n$. It is easy to see that

$$P_{n-1}[1] = Q_{n-1}[1] = L_n \quad \text{and} \quad R_{n-1}[1] = S_n.$$

Recently, the Pascal and generalized Pascal matrices and their properties have been studied by many authors; see for example [2,4,5,8,9]. Lü and Wang obtained the rules for the orders of the cyclic groups generated by reducing the $k-$generalized Fibonacci matrix modulo m [6].

For given a matrix $A = (a_{ij})$ with a_{ij}'s being integers, $A \pmod m$ means that every entry of A are reduced modulo m, that is, $A\ \ (mod\ m) = (a_{ij}\ \ (mod\ m))$. Let $\langle A\rangle_{p^a} = \left\{A^i \pmod{p^a} \middle| i \geq 0\right\}$ be the cyclic group generated by $A\ \ (mod\ p^u)$ and let $\left|\langle A\rangle_{p^a}\right|$ denote the order of $\langle A\rangle_{p^a}$. This paper discusses the multiplicative orders of the matrices $L_n,\ U_n,\ S_n,\ P_n[x],\ Q_n[x]$ and $R_n[x]$ modulo m where x is an integer satisfying certain divisibility hypotheses. In this paper, the usual notation p is used for a prime number.

2. Main results and proofs

Theorem 2.1. *Let $n (n \geq 2)$ be a positive integer and let G be either of the matrices U_n or L_n, and let m be a positive integer. Then the multiplicative order of $G \mod m$ is m.*

Proof. Let us consider the upper triangular matrix U_n. We prove this by direct calculation. Let $U_n = I_n + T_n$ where I_n is identity matrix of size n. Then the (i, j) entry of T_n will be

$$T_{i,j} = 0 \quad \text{if} \quad i \geq j,$$
$$T_{i,j} = \begin{pmatrix} j \\ i \end{pmatrix} \quad \text{if} \quad i < j.$$

It is easy to see by binomial theorem that

$$(U_n)^m = (I_n)^m + m\,(T_n) + \begin{pmatrix} m \\ 2 \end{pmatrix} (T_n)^2 + \cdots + (T_n)^m .$$

On the order hand the (i, j) entry of $(T_n)^m$ will be as follow:

If $m < n$, then $T_{ij} = 0$ for $i \geq j$ and $j = i + 1$ and $T_{ij} = \alpha.m$ for $i + 2 \leq j$, where $\alpha \in \mathrm{N}$.
If $m \geq n$, then $T_{ij} = 0$.

So, we get $m\,(T_n) + \begin{pmatrix} m \\ 2 \end{pmatrix} (T_n)^2 + \cdots + (T_n)^m \equiv 0_n \pmod{m}$ (where 0_n is zero matrix of size n).
Thus, writing U fort the matrix U_n, we obtain following:

$$\text{The } (i, j) \text{ entry of } U^m = \begin{cases} 0 & \text{if } i > j, \\ 1 & \text{if } i = j \end{cases}$$

and

$$\text{the } (i, j) \text{ entry of } U^m \equiv 0 \text{ if } i < j.$$

Then, we get $|\langle U_n \rangle_m| = m$.
The proof for the lower triangular matrix L_n is similar to the proof and is omitted. □

Theorem 2.2. *Let $n (n \geq 2)$ be a positive integer and let m be a positive integer. Then for the multiplicative orders of $S_n \mod m$ we have the following:*

(i) If $n = q^\alpha$ such that α is a positive integer and q is a prime number, then $\left|\langle S_n \rangle_{q^u}\right| = 3$ for $u = 1, 2$.
(ii)(a) If $\left|\langle S_n \rangle_{p^{v_1}}\right| = \left|\langle S_n \rangle_{p^{v_2}}\right|$ for $\forall v_1, v_2 \in [u_1, u_2]$ (where $[u_1, u_2] = \{x \in \mathrm{Z} : u_1 \leq x \leq u_2\}$), then $\left|\langle S_n \rangle_{p^{u_2+n}}\right| = p^n \left|\langle S_n \rangle_{p^{u_2}}\right|$.
(b) If $\left|\langle S_n \rangle_{p^{v_1}}\right| \neq \left|\langle S_n \rangle_{p^{v_2}}\right|$ for $\forall v_1, v_2 \in [u_1, u_2]$, then $\left|\langle S_n \rangle_{p^{u+n}}\right| = p^n \left|\langle S_n \rangle_{p^u}\right|$ for $\forall u \in [u_1, u_2]$.
(iii) If $m = \prod_{k=1}^{t} p_k^{e_k}$ $(t \geq 1)$ where p_k's are distinct primes, then $|\langle S_n \rangle_m|$=lcm$\left[\left|\langle S_n \rangle_{p_1^{e_1}}\right|, \left|\langle S_n \rangle_{p_2^{e_2}}\right|, \ldots, \left|\langle S_n \rangle_{p_t^{e_t}}\right|\right]$.

Proof. We prove the results by direct calculation. Let S_n be denoted by S.

(i) If $n = q^{\alpha}$ such that α is a positive integer and q is a prime number, then

$$\text{the } (i,j) \text{ entry of } S^3 = \begin{cases} q^2\varepsilon_1 \binom{i+j}{i} & \text{if } i<j, \\ q^2\varepsilon_2 \binom{i+j}{i} + 1 & \text{if } i=j, \\ q^2\varepsilon_3 \binom{i+j}{i} & \text{if } i>j, \end{cases}$$

where $q^2 \nmid \varepsilon_2 \binom{i+j}{i}$ for $i=j=0$ and ε_1, ε_2 and ε_3 are positive integers. Then, we have

$$q^2\varepsilon_1 \binom{i+j}{i} \equiv 0 \pmod{q^u} \quad \text{for } i<j \text{ and } u=1,2,$$
$$q^2\varepsilon_2 \binom{i+j}{i} + 1 \equiv 1 \pmod{q^u} \quad \text{for } i=j \text{ and } u=1,2,$$
$$q^2\varepsilon_3 \binom{i+j}{i} \equiv 0 \pmod{q^u} \quad \text{for } i>j \text{ and } u=1,2.$$

So, we get $\left|\langle S_n\rangle_{q^u}\right| = 3$ for $u=1,2$.

(ii)

(a) Let $\left|\langle S_n\rangle_{p^{v_1}}\right| = \left|\langle S_n\rangle_{p^{v_2}}\right| = a$ for $\forall v_1, v_2 \in [u_1,u_2]$. Then

$$\text{the } (i,j) \text{ entry of } S^a = \begin{cases} p^{u_2}\varepsilon_1^* \binom{i+j}{i} & \text{if } i<j, \\ p^{u_2}\varepsilon_2^* \binom{i+j}{i} + p^{u_2} & \text{if } i=j, \\ p^{u_2}\varepsilon_3^* \binom{i+j}{i} & \text{if } i>j, \end{cases}$$

where $p^{u_2} \nmid \varepsilon_2^* \binom{i+j}{i}$ for $i=j=0$ and ε_1^*, ε_2^* and ε_3^* are positive integers. By the routine multiplication it is easy to see that

$$\text{the } (i,j) \text{ entry of } S^{p^n a} = \begin{cases} p^{n+u_2}\varepsilon_1^\circ \binom{i+j}{i} & \text{if } i<j, \\ p^{n+u_2}\varepsilon_2^\circ \binom{i+j}{i} + p^{n+u_2} & \text{if } i=j, \\ p^{n+u_2}\varepsilon_3^\circ \binom{i+j}{i} & \text{if } i>j, \end{cases}$$

where $p^{n+u_2} \nmid \varepsilon_2^{\circ} \begin{pmatrix} i+j \\ i \end{pmatrix}$ for $i = j = 0$ and $\varepsilon_1^{\circ}, \varepsilon_2^{\circ}$ and ε_3° are positive integers. Then, we have

$$p^{n+u_2} \varepsilon_1^{\circ} \begin{pmatrix} i+j \\ i \end{pmatrix} \equiv 0 \pmod{p^{n+u_2}} \quad \text{for } i < j,$$
$$p^{n+u_2} \varepsilon_2^{\circ} \begin{pmatrix} i+j \\ i \end{pmatrix} + p^{n+u_2} \equiv 1 \pmod{p^{n+u_2}} \quad \text{for } i = j,$$
$$p^{n+u_2} \varepsilon_3^{\circ} \begin{pmatrix} i+j \\ i \end{pmatrix} \equiv 0 \pmod{p^{n+u_2}} \quad \text{for } i > j\ .$$

So, we get $\left| \langle S_n \rangle_{p^{u_2+n}} \right| = p^n \left| \langle S_n \rangle_{p^{u_2}} \right| = p^n.a$

(b) The proof is similar to the proof of ii'. and is omitted.

(iii) Let $m = \prod_{k=1}^{t} p_k^{e_k}$ $(t \geq 1)$ where p_k's are distinct primes and $\operatorname{lcm}\left[\left| \langle S_n \rangle_{p_1^{e_1}} \right|, \left| \langle S_n \rangle_{p_2^{e_2}} \right|, \ldots, \left| \langle S_n \rangle_{p_t^{e_t}} \right| \right] = \lambda$. Then, we have

$$\text{the } (i,j) \text{ entry of } S^{\lambda} = \begin{cases} \lambda \varepsilon_1' \begin{pmatrix} i+j \\ i \end{pmatrix} & \text{if } i < j, \\ \lambda m \varepsilon_2' \begin{pmatrix} i+j \\ i \end{pmatrix} + m & \text{if } i = j, \\ \lambda \varepsilon_3' \begin{pmatrix} i+j \\ i \end{pmatrix} & \text{if } i > j, \end{cases}$$

where $m \nmid \lambda \varepsilon_2' \begin{pmatrix} i+j \\ i \end{pmatrix}$ for $i = j = 0$ and ε_1', ε_2' and ε_3' are positive integers. Since $m | \lambda \varepsilon_1' \begin{pmatrix} i+j \\ i \end{pmatrix}, \lambda m \varepsilon_2' \begin{pmatrix} i+j \\ i \end{pmatrix}, \lambda \varepsilon_3' \begin{pmatrix} i+j \\ i \end{pmatrix}$, it is easy to see that

$$\lambda \varepsilon_1' \begin{pmatrix} i+j \\ i \end{pmatrix} \equiv 0 \pmod{m} \quad \text{for } i < j,$$
$$\lambda m \varepsilon_2' \begin{pmatrix} i+j \\ i \end{pmatrix} \equiv 1 \pmod{m} \quad \text{for } i = j,$$
$$\lambda \varepsilon_3' \begin{pmatrix} i+j \\ i \end{pmatrix} \equiv 0 \pmod{m} \quad \text{for } i > j\ .$$

So, we get $|\langle S_n \rangle_m| = \operatorname{lcm}\left[\left| \langle S_n \rangle_{p_1^{e_1}} \right|, \left| \langle S_n \rangle_{p_2^{e_2}} \right|, \ldots, \left| \langle S_n \rangle_{p_t^{e_t}} \right| \right]$. □

S_n mod p is an element of the finite general linear group $GL\,(n, p)$. The lower triangular matrices with 1 on the diagonal form a Sylow p-subgroup Q of order p^k, where $k = \frac{n(n-1)}{2}$. Since, for N a nilpotent $n \times n$ matrix, $N^n = 0$, the binomial theorem implies that the order of each element of Q divides p^r, where r is the least integer greater than equal to $\log_p(n)$. Each semi-simple element of $GL\,(n, p)$ is the direct sum of irreducible elements each of which has order dividing $p^s - 1$ for some positive integer $s \leq n$. Since every element of $GL\,(n, p)$ is conjugate to the product AB of an element A

Table 1
The orders of the cyclic groups $\langle S_3\rangle_p$ and $\langle S_6\rangle_p$.

p	$\lvert\langle S_3\rangle_p\rvert$	$\lvert\langle S_6\rangle_p\rvert$	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p^\sigma$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-p^\sigma$
7	6	12	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p^2$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-p^4$
11	10	12	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-p^4$
13	7	78	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-p^5$
17	16	34	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p^2$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-p^5$
67	33	902292	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p^2$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-1$
97	98	912672	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-p^3$
163	9	5022	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p^2$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-p$
179	178	2867669	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p^2$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-p^3$
241	120	3513961	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p^2$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-p^2$
733	367	268644	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-p^4$
1033	1034	1102302938	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-1$
3163	1581	5274075291	$\lvert\langle S_3\rangle_p\rvert \mid p^3-p^2$	$\lvert\langle S_6\rangle_p\rvert \mid p^6-p^3$

of Q and a semi-simple element B which commutes with A, so that the order of AB is the product of the orders of A and B, it follows that the order of AB divides $p^r\mathrm{lcm}\left\{\left(p^{s(i)}-1\right) : s(i) \text{ are the degrees of the irreducible components of } B\right\}$. We now conjecture a more restrictive bound on the order of $S_n \pmod p$.

Conjecture 2.1. *If $p \geq n$, then there exists at least an integer σ with $0 \leq \sigma \leq n-1$ such that $\left|\langle S_n\rangle_p\right|$ divides $(p^n - p^\sigma)$.*

Table 1 lists some primes for which the conjecture is true when $n = 6$ and $n = 3$.

Theorem 2.3. *Let $n(n \geq 2)$ be a positive integer and let m be a positive integer, and let $x = \prod_{k=1}^{\ell} q_k^{e_k}$ $(\ell \geq 1)$ where q_k's are distinct primes. Then for the multiplicative orders of $P_n[x] \mod m$ for $x \geq 2$ we have the following:*

(i) $\left|\langle P_n[x]\rangle_{q_u^{e_u}}\right| = 1$ *for* $u \in [1, \ell]$.
(ii) If w is a positive integer such that $w > e_1, \ldots, e_\ell$, then $\left|\langle P_n[x]\rangle_{q_u^{w}}\right| = q_u^{w-e_u}$ *for* $u \in [1, \ell]$.
(iii) If θ is a positive integer and $p \neq q_1, \ldots, q_l$, then $\left|\langle P_n[x]\rangle_{p^\theta}\right| = p^\theta$.
(iv) If $m = \prod_{k=1}^{t} p_k^{e_k} (t \geq 1)$ where p_k's are distinct primes, then $\left|\langle P_n[x]\rangle_m\right| = \mathrm{lcm}\left[\left|\langle P_n[x]\rangle_{p_1^{e_1}}\right|, \left|\langle P_n[x]\rangle_{p_1^{e_1}}\right|, \ldots, \left|\langle P_n[x]\rangle_{p_t^{e_t}}\right|\right]$.

Proof. We prove the results by direct calculation.

(i) Since $q_u^{e_u} \mid x$ for $u \in [1, \ell]$, we have

$$P_n(x; i, j) = 0 \quad \text{for } i < j,$$
$$P_n(x; i, j) = 1 \quad \text{for } i = j,$$
$$P_n(x; i, j) = x^{i-j}\begin{pmatrix} i \\ j \end{pmatrix} \equiv 0 \pmod{q_u^{e_u}} \quad \text{for } i > j.$$

So, we get $\left|\langle P_n[x]\rangle_{q_u^{e_u}}\right| = 1$ for $u \in [1, \ell]$.

(ii) If u and w are positive integers such that $w > e_1, \ldots, e_\ell$, and $u \in [1, \ell]$, then

$$P_n\,(x; i, j)^{q_u^{w-e_u}} = 0 \quad \text{for } i < j,$$
$$P_n\,(x; i, j)^{q_u^{w-e_u}} = 1 \quad \text{for } i = j,$$
$$P_n\,(x; i, j)^{q_u^{w-e_u}} = q_u^{w-e_u}\eta_1 x^{i-j}\begin{pmatrix} \mathrm{i} \\ \mathrm{j} \end{pmatrix} \equiv 0 \left(\bmod\ q_u^{w}\right) \quad \text{for } i > j,$$

where η_1 is a positive integer. So, we get $\left|\langle P_n\,[x]\rangle_{q_u^w}\right| = q_u^{w-e_u}$.

(iii) If θ is a positive integer and $p \neq q_1, \ldots, q_l$, then

$$P_n\,(x; i, j)^{p^\theta} = 0 \quad \text{for } i < j,$$
$$P_n\,(x; i, j)^{p^\theta} = 1 \quad \text{for } i = j,$$
$$P_n\,(x; i, j)^{p^\theta} = p^\theta \eta_2 x^{i-j}\begin{pmatrix} \mathrm{i} \\ \mathrm{j} \end{pmatrix} \equiv 0 \left(\bmod\ p^\theta\right) \quad \text{for } i > j,$$

where η_2 is a positive integer. So, we get $\left|\langle P_n\,[x]\rangle_{p^\theta}\right| = p^\theta$.

(iv) The proof is similar to the proof of Theorem 2.2(iii) and is omitted. □

Theorem 2.4. *Let $n (n \geq 2)$ be a positive integer and let G be either of the matrices $Q_n\,[x]$ or $R_n\,[x]$, and let m be a positive integer. Then the multiplicative order of G mod m for $x \geq 2$ are as follows:*

(i) Let $(p, x) = 1$.
(i') If $\left|\langle G\rangle_{p^{v_1}}\right| = \left|\langle G\rangle_{p^{v_2}}\right|$ for $\forall v_1, v_2 \in [u_1, u_2]$, then $\left|\langle G\rangle_{p^{u_2+n}}\right| = p^n \left|\langle G\rangle_{p^{u_2}}\right|$.
(i'') If $\left|\langle G\rangle_{p^{v_1}}\right| \neq \left|\langle G\rangle_{p^{v_2}}\right|$ for $\forall v_1, v_2 \in [u_1, u_2]$, then $\left|\langle G\rangle_{p^{u+n}}\right| = p^n \left|\langle G\rangle_{p^{u}}\right|$ for $\forall u \in [u_1, u_2]$.
(ii) If $(m, x) = 1$ and $m = \prod_{k=1}^{t} p_k^{e_k} (t \geq 1)$ where p_k's are distinct primes, then $|\langle G\rangle_m| = \operatorname{lcm}\left[\left|\langle G\rangle_{p_k^{e_1}}\right|, \left|\langle G\rangle_{p_k^{e_2}}\right|, \ldots, \left|\langle G\rangle_{p_k^{e_t}}\right|\right]$.

Proof. The proofs of (i) and (ii) are similar to the proofs of Theorem 2.2(ii) and Theorem 2.2(iii) respectively and are omitted. □

Conjecture 2.2. *If $(p, x) = 1$ and $\left|\langle Q_n\,[x]\rangle_p\right| < p$, then $\left|\langle Q_n\,[x]\rangle_p\right|$ divides $(p - 1)$.*

Table 2
The orders of the cyclic groups $\langle Q_2[6]\rangle_p$ and $\langle Q_4[6]\rangle_p$.

p	$\langle Q_2[6]\rangle_p$	$\lvert\langle Q_4[6]\rangle_p\rvert$	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$
11	5	5	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$
37	2	2	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$
167	83	83	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$
733	366	366	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$
937	13	13	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$
1709	427	427	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$
3163	1581	1581	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$
4177	348	348	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$
28751	14375	14375	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$
77863	2049	2049	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$
457903	228951	228951	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$
999983	499991	499991	$\lvert\langle Q_2[6]\rangle_p\rvert \mid p-1$	$\lvert\langle Q_4[6]\rangle_p\rvert \mid p-1$

Table 3
The orders of the cyclic groups $\langle R_2[6]\rangle_p$ and $\langle R_4[6]\rangle_p$.

p	$\lvert\langle R_2[6]\rangle_p\rvert$	$\lvert\langle R_4[6]\rangle_p\rvert$	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p^\sigma$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-p^\sigma$
7	6	16	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p^3$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-p$
11	40	3221	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p^2$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-p$
13	168	15372	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p^2$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-1$
19	180	360	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p^2$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-p^4$
29	6097	840	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-p^4$
37	36	374832	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p^3$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-p^2$
41	34460	120610	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-1$
97	152112	8656593	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-p$
179	178	344120280	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p^3$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-1$
317	316	4550716	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p^3$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-p^3$
907	453	677497518936	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p^3$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-1$
1277	520610233	3395896820230151	$\lvert\langle R_2[6]\rangle_p\rvert \mid p^4-p$	$\lvert\langle R_4[6]\rangle_p\rvert \mid p^6-p$

Conjecture 2.3. *If* $(p, x) = 1$ *and* $\left|\langle Q_{n_1}[x]\rangle_p\right|, \left|\langle Q_{n_2}[x]\rangle_p\right| < p$, *then* $\left|\langle Q_{n_1}[x]\rangle_p\right| = \left|\langle Q_{n_2}[x]\rangle_p\right|$.

Table 2 lists some primes for which Conjectures 2.2 and 2.3. are true $n = 2,\ 4$ and $x = 6$.

Conjecture 2.4. *If* $(p, x) = 1$ *and* $p \geq n + 1$, *then there exists at least an integer* σ *with* $0 \leq \sigma \leq n + 1$ *such that* $\left|\langle R_n[x]\rangle_p\right|$ *divides* $\left(p^{n+2} - p^\sigma\right)$.

Table 3 lists some primes for which the conjecture is true $n = 2,\ 4$ and $x = 6$.

Acknowledgment

The authors thank the referee for her/his valuable suggestions which improved the presentation of the paper. This Project was supported by the Commission for the Scientific Research Projects of Kafkas Univertsity. The Project No. 2010-FEF-61.

References

[1] A. Edelman, G. Strang, Pascal matrices, MIT, Cambridge, MA, 2003.
[2] E. Kılıç, N. Ömür, G. Tatar, Y.T. Ulutaş, Factorizations of the Pascal matrix via a generalized second order recurrent matrix, Hacet. J. Math. Statist. 39 (2) (2009) 305–316.
[3] G.S. Call, D.J. Velleman, Pascal's matrices, Amer. Math. Monthly 100 (1993) 372–376.
[4] G.S. Cheon, J.S. Kim, Stirling matrix via Pascal matrix, Linear Algebra Appl. 329 (2001) 45–59.
[5] G.V. Lee, S.U. Cho, The generalized Pascal matrix via Fibonacci matrix and generalized Pell matrix, J. Korean Math. Soc. 42 (2) (2008) 479–491.
[6] K. Lü, J. Wang, k-Step Fibonacci sequence modulo m, Util. Math. 71 (2007) 169–178.
[7] Pascal matrix. October 2010. Available from: <http://en.wikipedia.org/wiki/Pascal_matrix>.
[8] R. Brawer, M. Pirovino, Linear algebra of the Pascal matrix, Linear Algebra Appl. 174 (1992) 13–23.
[9] T.B. Deng, S. Chivapreecha, K. Dejhan, Generalized Pascal matrices and inverses using one-to-one rational polynomial s–z transformations, in: The 23rd International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2008).
[10] Z. Tang , R. Duraiswami, N. Gumerov, Fast algorithms to compute matrix–vector products for Pascal matrices, Technical Reports from UMIACS, 2004.
[11] Z. Zhizheng, The linear algebra of the generalized Pascal matrix, Linear Algebra Appl. 250 (1997) 51–60.